What is claimed is:

1. A computerized method for collecting suspected data of interest from a computer that includes short-term memory and long-term memory, wherein the suspected data of interest resides within the short-term memory and is expected to be characteristic of an operating system exploit, said computerized method comprising:

(a) searching the short-term memory to locate at least one target memory range therein which contains the suspected data of interest; and

(b) copying the suspected data of interest within the target memory range to an alternate data storage location, in a manner which avoids writing the suspected data to the long-term memory.

2. A computerized method according to claim 1 wherein said alternate data storage location is external to the computer.

3. A computerized method according to claim 2 wherein said alternate data storage location has an associated long-term memory.

4. A computerized method according to claim 1 wherein said alternate data storage location is a removable, non-volatile memory media.

5. A computerized method according to claim 1 comprising preliminarily halting all unnecessary processes on the computer and remounting the computer's file system in read-only mode.

6. A computerized method according to claim 1 comprising halting the computer's CPU after the suspected data of interest has been copied.

7. A computerized method according to claim 1 whereby the suspected data of interest corresponds to one or more from a group consisting of: information associated with hidden kernel modules, re-routed system call table addresses, information within dynamic kernel memory, information associated with a running kernel image, and process information associated with each running process on the computer.

8. A computerized method according to claim 1 whereby the suspected data of interest includes information associated with each loaded kernel module, and whereby locating the target memory range comprises searching dynamic kernel memory to ascertain a corresponding memory range for each loaded kernel module.

9. A computerized method according to claim 8 comprising copying associated module data from each corresponding memory range to the alternate data storage

location, thereby to obtain a respective image associated with each loaded kernel module.

10. A computerized method according to claim 1 whereby the suspected data of interest corresponds to system call table information, and whereby locating the target memory range comprises scanning the system call table to identify an address associated with each function call therein.

11. A computerized method according to claim 10 comprising copying an identification of each said address onto the alternate data storage location.

12. A computerized method according to claim 11 comprising copying to the alternate data storage location an associated range of kernel dynamic memory corresponding to each function call address which is outside of the kernel's static memory range.

13. A computerized method according to claim 1 comprising copying a running image of the computer's kernel to the alternate data storage location.

14. A computerized method according to claim 1 whereby the suspected data of interest includes process information associated with each running process on the computer.

15. A computerized method according to claim 14 for use with a computer running a Linux operating system, whereby said process information is one or more types of process-related data selected from a group consisting of: an executable image from the computer's file system corresponding to the running process, an executable image from memory for the running process, each file descriptor opened by the running process, an environment for the running process, each shared library mapping associated with the running process, command line data used to initiate the running process, and each mount point created by the running process.

16. A computerized method for collecting target forensics data from a computer that includes a volatile memory and a non-volatile memory, wherein the target forensics data resides within the volatile memory and is characteristic of a type of exploitation to the computer's operating system which renders the operating system insecure, said computerized method comprising:

(a) locating the target forensics data within the volatile memory; and

(b) copying the target forensics data from the volatile memory to an alternate data storage location in a manner which avoids utilizing memory resources associated with the non-volatile memory.

17. A computerized method for collecting suspected data of interest from a computer that includes volatile memory and non-volatile memory, wherein the suspected data of interest resides within the volatile memory and is expected to be characteristic of an operating system exploit, said computerized method comprising:

(a) locating at least one target memory range containing the suspected data of interest; and

(b) copying the suspected data of interest from the target memory range to a previously unused data storage location while preserving integrity of memory resources within the non-volatile memory.

18. A computerized method for collecting suspected data of interest from a computer that includes short-term memory and long-term memory, wherein the suspected data of interest resides within the short-term memory and is expected to be characteristic of an operating system exploitation which has rendered the computer insecure, said computerized method comprising:

(a) identifying different types of suspected data of interest, each of which is expected to be characteristic of said exploitation, thereby to establish a target data set; and

(b) for each type of suspected data of interest within the target data set:

(i) searching the short-term memory to locate an associated target memory range therein which contains the suspected data of interest; and

(ii) copying the suspected data of interest within the associated target memory range to an alternate data storage location, in a manner which avoids writing the suspected data to the long-term memory.

19. A computer-readable medium for use in collecting suspected data of interest residing within a computer's short-term memory, wherein the suspected data of interest is expected to be characteristic of an operating system exploit, said computer-readable medium having executable instructions for performing a method, comprising:

(a) locating at least one target memory range within the short-term memory which contains the suspected data of interest; and

(b) enabling the suspected data of interest to be copied from the target memory range to an alternate data storage location, in a manner which avoids writing the suspected data of interest to any long-term memory region of the computer.

20. A computer-readable medium having executable instructions for performing a method according to claim 19 wherein said alternate data storage location has associated long-term memory.

21. A computer-readable medium having executable instructions for performing a method according to claim 19 wherein said alternate data storage location is a removable storage device.

22. A computer-readable medium having executable instructions for performing a method according to claim 19 comprising preliminarily halting all unnecessary processes on the computer and remounting the computer's file system in read-only mode, and subsequently halting the computer's CPU after the suspected data of interest has been copied.

23. A computer-readable medium having executable instructions for performing a method according to claim 19 whereby the suspected data of interest corresponds to one or more from a group consisting of: information associated with hidden kernel modules, re-routed system call table addresses, information within dynamic kernel memory, information associated with a running kernel image, and process information associated with each running process on the computer.

24. A computer-readable medium having executable instructions for performing a method according to claim 19 whereby the suspected data of interest includes information associated with each loaded kernel module, and whereby locating the target memory range comprises searching dynamic kernel memory to ascertain a corresponding memory range for each loaded kernel module.

25. A computer-readable medium having executable instructions for performing a method according to claim 24 comprising copying associated module data from each corresponding memory range to the alternate data storage location, thereby to obtain a respective image associated with each loaded kernel module.

26. A computer-readable medium having executable instructions for performing a method according to claim 19 whereby the suspected data of interest corresponds to system call table information, and whereby locating the target memory range

comprises scanning the system call table to identify an address associated with each function call therein.

27. A computer-readable medium having executable instructions for performing a method according to claim 26 comprising copying an identification of each said address onto the alternate data storage location.

28. A computer-readable medium having executable instructions for performing a method according to claim 26 comprising copying to the alternate data storage location an associated range of kernel dynamic memory corresponding to each function call address which is outside of the kernel's static memory range.

29. A computer-readable medium having executable instructions for performing a method according to claim 19 comprising copying a running image of the computer's kernel to the alternate data storage location.

30. A computer-readable medium having executable instructions for performing a method according to claim 19 whereby the suspected data of interest includes process information associated with each running process on the computer.

31. A computer-readable medium having executable instructions for performing a method according to claim 30 for use with a computer running a Linux operating system, whereby said process information is one or more types of process-related data selected from a group consisting of: an executable image from the computer's file system corresponding to the running process, an executable image from memory for the running process, each file descriptor opened by the running process, an environment for the running process, each shared library mapping associated with the running process, command line data used to initiate the running process, and each mount point created by the running process.

32. A system for collecting target forensics data expected to be characteristic of an operating system exploitation, comprising:

(a) a short-term memory for temporary data storage;

(b) a long-term memory for permanent data storage;

(c) a data storage location distinct from said short-term memory and said long-term memory, and

(d) a processor programmed to:

locate a target memory range within short term-memory which contains the target forensics data; and

copy the target forensics data from the target memory range to the data storage location in a manner which avoids writing said forensics data to the long-term memory.

33. A system according to claim 32 including at least one random access memory (RAM) device for accommodating said temporary data storage, and at least one hard drive adapted to accommodate both permanent data storage and needed temporary data storage.